

Forensic Readiness for Effective Incident Management

Abstract

Banking and financial institutions today face several information security related threats. There is a visible surge in cyber-attacks, which is leading to an increase in issues related to legal, regulatory, and privacy compliance. The lack of proper forensic readiness also pushes up the cost of investigation of cyber security incidents and results in legal and compliance issues for organizations. The ability to identify, investigate, and mitigate such security incidents, while ensuring legal and regulatory compliance, has thus become an organizational imperative. This paper discusses the components of an effective forensic readiness program, the implementation strategy, and the costs involved, while highlighting potential benefits.

Cyber-attacks: A growing area of concern

The recent cyber-attacks on banks, financial institutions, and payment processors are a validation of the increasing technical expertise of cybercriminals and their ability to cause significant damage while orchestrating remotely. From mobile malware to banking Trojans, and point-of-sale (POS) and retail breaches, the threat landscape continues to evolve. At the same time, payment risks associated with retailers and payment processors are raising concerns. POS breaches, such as the ones that struck Target Corporation and Neiman Marcus, illustrate the complexities involved in ensuring the security of financial transactions across multiple entities. Distributed Denial of Service (DDoS) attacks, spear phishing, mobile malware, ransomware, and insider threats, continue to endanger banking and financial institutions. Given the circumstances, an ideal approach is to focus on detecting, recovering, and mitigating cyber security risks across multiple channels. A poorly managed security incident can adversely impact an organization by increasing downtime, escalating the cost of investigation, and attracting legal liability and sanctions besides resulting in negative publicity.

How should banks and financial institutions prepare themselves to deal with such security incidents and avoid negative consequences such as cost of investigation, litigation, and business downtime? The solution lies in deploying a digital forensic readiness program.

How Digital Forensic Readiness Can Come to the Rescue

Forensic science is the application of science and technology to resolve legal problems. Digital forensics is a branch of forensic science that deals with acquiring, authenticating, and analyzing digital evidence in a legally acceptable manner. Digital forensics is commonly employed as a post security incident response to understand the 'what, why, who, where, and when' of an incident, but can come in handy as a preemptive tool as well. Organizations can hugely benefit from collecting, authenticating, and preserving the evidence before the occurrence of an incident. The forensic readiness concept essentially implies collecting credible digital evidence and minimizing the investigation cost during an incident response. It also covers an organization's ability to use digital evidence to its maximum potential while reducing the cost of investigation.

Our experience indicates that the average cost of investigation and cleanup activities following a security incident has increased manifold over the last few years. This increase is mainly attributed to a lack of readiness to identify, collect, and analyze proper evidence to mitigate the impact of cyber-attacks.

Digital forensics has moved from a reactive to a proactive practice and has become an integral part of information security.

Case in Point

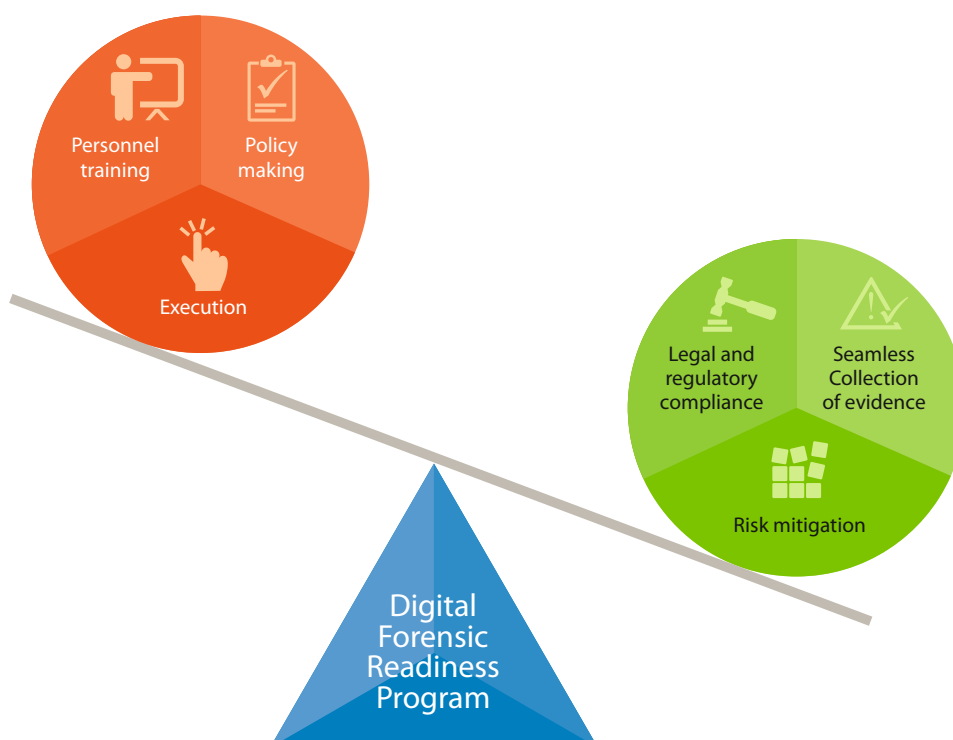
In response to a money laundering investigation, a leading bank was asked to produce relevant digital evidence by the law enforcement agencies. Additionally, the banking regulatory authority issued the bank a notice to conduct a third party investigation and submit a report. To maintain its reputation and safeguard the interests of its stakeholders, the bank engaged with a service provider to investigate and identify the modus operandi of the incident, violation of KYC norms if any, status of security controls, and so on. The absence of a holistic forensic readiness program made it impossible for the bank to produce the digital evidence required for investigation and electronic evidence which can stand to the scrutiny of court leading to penalties to the tune of USD 1.25 million, and a significant investigation cost as well.

To prevent recurrence of such incidents, we advised the bank to deploy sound data collection, retention and retrieval policies, such as electronic discovery service to analyze different types of data available on the bank's servers.

A Cost versus Benefit Analysis of a Digital Forensic Readiness Program

Some typical costs related to the implementation of a digital forensic readiness program arise from:

- **Policy making:** The organization's data collection and retention, cyber security and incident response policies and procedures should be evaluated and updated accordingly. Assessing the incident response maturity of the organization is a prerequisite.
- **Execution:** A seamless mechanism for collecting, storing, retrieving, and retaining digital evidence, needs to be deployed. In addition, advanced analytics capabilities need to be built in to the system.
- **Personnel training:** Employees need to be trained on information security management, security awareness, incident response, and digital forensic capability.



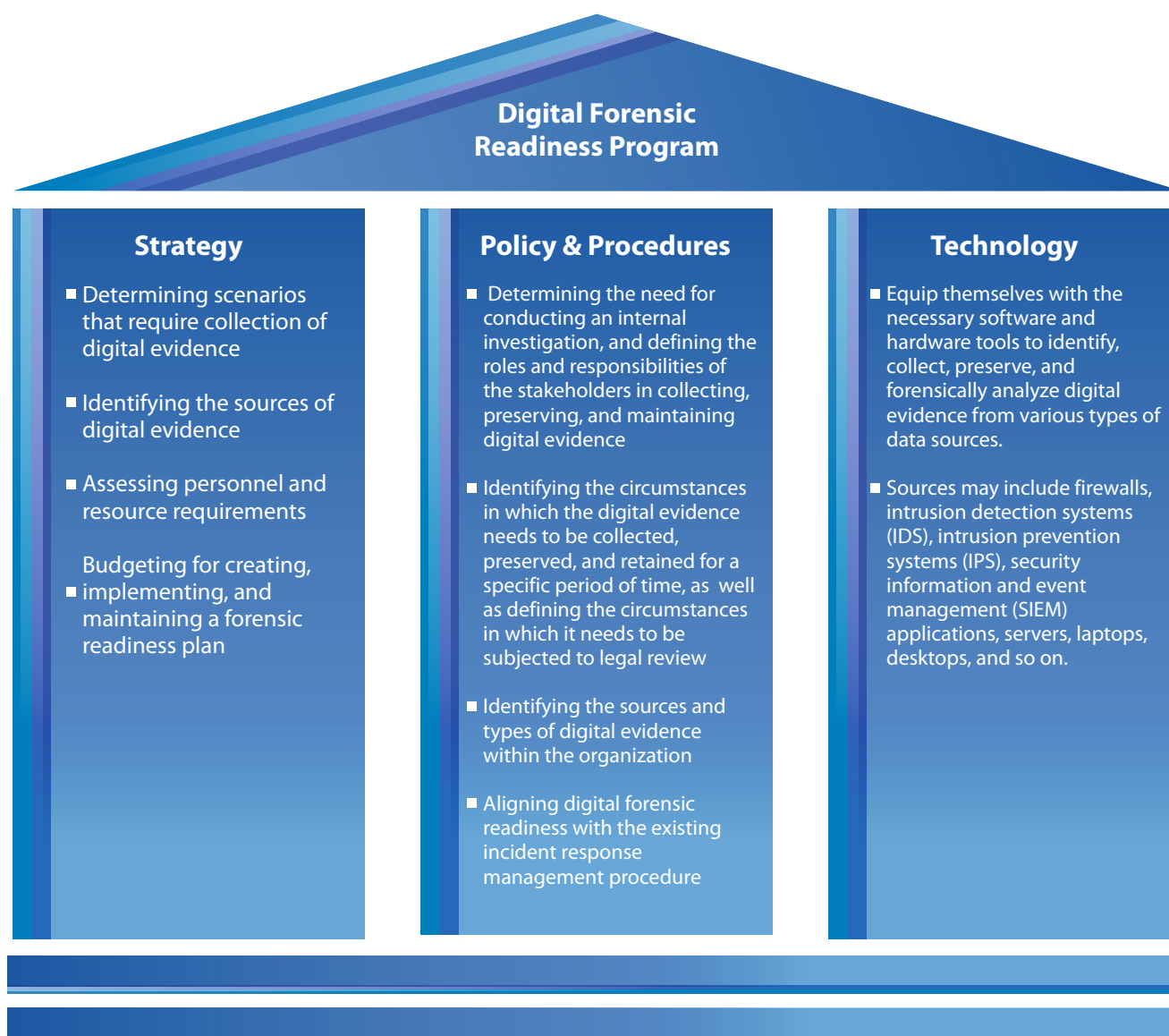
Digital forensic readiness offers benefits across multiple business operations, such as:

- **Seamless collection of evidence:** The program enables organizations to gather evidence in a legally acceptable manner, and without disrupting business processes. It also ensures that the collected evidence is relevant to the case, thus having a positive impact on the outcome of the investigation.
- **Risk mitigation:** Accurate identification of location of potential digital evidence helps organizations decrease the impact of cyber security incidents. Business downtime and investigation costs can be significantly reduced.
- **Legal and regulatory compliance:** The program helps organizations ensure requisite legal compliance, thus building a positive image among customers, which in turn increases their confidence during contractual discussions. It also enables effective management of litigation issues or when the court orders for the investigation data to be presented.

In a nutshell, the benefits of implementing a forensic readiness program clearly outweigh the costs associated with it.

Components of a Digital Forensic Readiness Program

The three pillars of a digital forensic readiness program are strategy, policy and procedures, and technology.



Conclusion

Banking and financial institutions no longer view cyber security as a financial burden or a compliance hurdle, but consider it a vital business enabler that enhances customer confidence and brings in more business. As a result, organizations' attitude to cyber security investments has changed. Organizations should extend this shift to forensic readiness programs as well to better respond to security incidents and mitigate their impact. By integrating an effective digital forensic readiness framework with the information security and governance strategy, organizations can minimize the cost of collecting evidence in a forensically sound manner besides reducing litigation and business downtime.

About the Author

Krishna Sastry Pendyala

Krishna Sastry Pendyala heads the Fraud Management and Digital Forensics group with the Enterprise Security and Risk Management (ESRM) unit at Tata Consultancy Services (TCS). With over 23 years of experience in this field, Krishna has played a pivotal role in safeguarding critical national information infrastructure, proactively and reactively, against cyber threats. Before joining TCS, he worked with the Ministry of Home Affairs, Govt. of India, as a digital forensic investigator where he managed cyber security incidents and crime investigations of national and international importance.

About TCS' Banking and Financial Services Business Unit

With over four decades of experience working with the world's leading banks and financial institutions, TCS offers a comprehensive portfolio of domain-focused processes, frameworks, and solutions that empower organizations to respond to market changes quickly, manage customer relationships profitably, and stay ahead of competition. Our offerings combine customizable solution accelerators with expertise gained from engaging with global banks, regulatory and development institutions, and diversified and specialty financial institutions.

TCS ranked #2 in the 2013 FinTech 100 rankings of top global technology providers to the financial services industry and counts 12 of the top 20 global financial institutions among its clientele. From retail and corporate banking, capital markets, market infrastructure, and cards, to risk management and treasury, TCS helps organizations achieve key operational and strategic objectives.

About TCS Enterprise Security and Risk Management (ESRM) Unit

Leveraging our rich experience in enterprise security, TCS helps global enterprises across verticals manage risks, ensure regulatory compliance, proactively protect critical information assets against emerging threats, achieve resilience, and recover rapidly from security incidents.

TCS has a successful track record of executing numerous engagements globally, delivering domain integrated security solutions fully aligned with clients' objectives. Our global service infrastructure, including the shared services Security Operations Center (SOC) and Forensics Labs, backed by the capabilities of our certified security consultants, make TCS a strategic partner of choice for nearly half of the Fortune 500 companies.

Our Security Innovation labs foster research and innovation in the field of data privacy, and have yielded multiple patents and intellectual properties in data protection and cryptographic products. We leverage our alliances with all major security vendors, including IBM, CISCO, and Oracle, to deliver end-to-end services and solutions across the security landscape, from consulting to implementation and managed services.

Contact

For more information about TCS' Banking and Financial Services or ESRM, email us at bfs.marketing@tcs.com global.esrm@tcs.com

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match.

TCS offers a consulting-led, integrated portfolio of IT and IT-enabled infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com

IT Services
Business Solutions
Consulting